NCA
National Crime Agency

October 2024

Evil Corp: Behind the Screens

Who are Evil Corp?

Evil Corp (also known as Indrik Spider) originated from Russia and are the most pervasive cybercrime group to ever have operated. Maksim Yakubets, who also goes by the online alias 'Aqua' and has a $5 million bounty for his arrest, was Evil Corp's founder and led the group for the majority of its lifespan.

One of the first major financial cybercrime groups, Evil Corp developed a series of malware and ransomware strains which have caused significant harm to numerous organisations and sectors, including healthcare, critical national infrastructure and government.

Several law enforcement and government operations have taken place to disrupt the group since its formation, most notably in the form of sanctions and indictments in December 2019. As a result, the group have been forced to scrap their modus operandi, and attempt new tactics to evade the additional scrutiny and restrictions put on them.

Characterised by their longevity, adaptability, organisational hierarchy and close links with the Russian state, Evil Corp have proved a persistent threat for over a decade, and members continue to operate within the Russian Federation. However, since late-2019, their success and influence in the cybercrime ecosystem have dwindled.

This paper provides a high level overview of the group's origins, operations and evolution.

With thanks to CrowdStrike, Intel471 and QIntel for their support.

The Evil Corp Group

The majority of organised cybercrime groups operate predominately online, but Maksim Yakubets' Evil Corp was a more personal affair: a family-centred operation based in Moscow, reminiscent of a traditional organised crime gang.

The Yakubets family were no strangers to financial crime: Viktor Yakubets, father of Maksim, had significant historical ties to money laundering activity. Maksim took this family business into the 21st century, branching into cybercrime and bringing his father, brother (Artem) and cousins (Kirill and Dmitry Slobodskoy) along with him.

By drawing on this family knowledge, Evil Corp became experts in laundering the proceeds of their cybercriminal activities. Highly organised, a huge amount of resource was invested in professionalising their business, whether that be by managing money mule networks, cryptocurrency trading, setting up front companies or employing lawyers. Although their technical capabilities were advanced, it was arguably their ability to realise the proceeds of their cybercrime that made them so successful.

At their peak, Evil Corp were a tight knit group, operating out of physical office locations in Moscow (including Chianti Café and Scenario Café), and spending a lot of time socialising together, along with their wives and girlfriends. They even went on group holidays.

Maksim was the leader of the group, making all of the important decisions and keeping a firm grip on their activities. He was careful about exposing different group members to different areas of the business, even keeping details of his work secret from his wife.

However, he clearly placed a lot of trust in his long-term associate and second in command, Aleksandr Ryzhenkov. Yakubets started working with Ryzhenkov around 2013 whilst they were both still involved in The Business Club. The partnership endured, and they worked together on a number of Evil Corp's most prolific ransomware strains.

At least $300m extorted from victims worldwide

Victims from sectors including healthcare and government

10 years In operation for over a decade

Cyber Proxies: Evil Corp and the Russian State

Whilst most cybercriminal activity is financially motivated, the Russian Intelligence Services have in some reported cases directed cybercriminals to conduct malicious cyber activity, or used malware strains for espionage purposes. For example, in 2017, two Russian FSB officers were indicted by the US Department of Justice (DoJ) for directing criminal hackers to compromise 500 million Yahoo accounts. Another notable Russian cybercriminal, Vitaly Kovalev, who was sanctioned by the UK and US governments in 2023 for his senior role in the Trickbot cybercrime group, also had a relationship with the Russian Intelligence Services.

Evil Corp held a privileged position, and the relationship between the Russian state and this cybercriminal group went far beyond the typical state-criminal relationship of protection, payoffs and racketeering. In fact, prior to 2019, Evil Corp were tasked by Russian Intelligence Services to conduct cyber-attacks and espionage operations against NATO allies.

Liaison with the intelligence services was led by Maksim Yakubets. As Evil Corp evolved, he became the group's main contact with Russian officials, developing or seeking to develop relationships with FSB, SVR and GRU officials. Multiple other members of the Evil Corp group have their own ties with the Russian state. In particular, Yakubets' father-in-law, Eduard Benderskiy, was a key enabler of Evil Corp's state relationships.

Eduard Benderskiy is a former high ranking official of the FSB's secretive 'Vympel' unit and now owns various organisations carrying the 'Vympel' name. It has been reported by Bellingcat that through Vympel, Benderskiy has been involved in multiple overseas assassinations on behalf of the Russian state. Evidently, he is a highly connected individual still closely involved with the Kremlin's activities.

Benderskiy leveraged his status and contacts to facilitate Evil Corp developing relationships with officials from the Russian Intelligence Services. After the US sanctions and indictments against Evil Corp members in December 2019, Benderskiy used his extensive influence to protect the group, both by providing senior members with security and by ensuring they were not pursued by internal Russian authorities.

Evil Corp's Evolution

Jabber Zeus Crew

Jabber Zeus

2009

2010
Law enforcement **arrest** members of Jabber Zeus Crew

2011

The Business Club

2014

Law enforcement **takedown** of GameOverZeus

GameOverZeus

Evil Corp

Dridex

BitPaymer

2017

2019

Evil Corp **Splits**

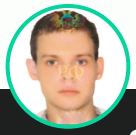
DoppelPaymer

US **Sanctions** and law enforcement **indictments**

WastedLocker

Hades
PhoenixLocker
PayloadBIN
Macaw

Evil Corp used **LockBit** Ransomware as a Service



2022

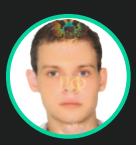
2024

International **sanctions** and law enforcement **indictment** against members of Evil Corp

Action Taken Group Malware

Maksim YAKUBETS

Igor TURASHEV



Aleksandr RYZHENKOV

Timeline of Evil Corp's Activity

2007-2011: The Early Days

- Maksim Yakubets, leader of the Evil Corp OCG, probably began his involvement in cybercrime activity around 2007.
- Since at least 2009, Yakubets worked with several notorious cybercriminals including Evgeniy Bogachev and Vitaliy Kovalev (involved in Dyre, Trickbot and Conti) to deploy malware.

2011-2014: The Business Club

- A number of Russian-speaking cybercriminals, including Maksim Yakubets and Vitaliy Kovalev, came together to form The Business Club cybercrime group. Yakubets would later team up with other members, Igor Turashev and Aleksandr Ryzhenkov, in Evil Corp.
- Aleksandr Ryzhenkov was part of an affiliate group of The Business Club which specialised in bank transfer fraud against the UK.

2014: Dridex and the Formation of Evil Corp as an OCG

- Maksim Yakubets worked with Aleksandr Ryzhenkov and other former members of The Business Club to create Dridex malware.
- Dridex was brought into operation in June 2014 and went on to become one of the most prolific and successful banking malware strains to date. The group set up the domain Ev17corp.biz to coordinate their operations, and Evil Corp was born.
- Much like current Ransomware as a Service (RaaS) models, Evil Corp segmented and rented out the Dridex botnet to affiliates who could use it for their own malicious cyber operations.

2017-2018: BitPaymer - The Group Begins Using Ransomware

- In mid-2017, Evil Corp used Dridex to start deploying ransomware. BitPaymer was used in a number of big game hunting attacks, targeting high value or high profile organisations.

2019-2020: The Split - DoppelPaymer

- After an acrimonious split between Maksim Yakubets and another key Evil Corp member, Igor Turashev (beginning in mid-2019 but exacerbated by the December 2019 disruption), the group divided and Turashev led the development of DoppelPaymer ransomware. DoppelPaymer was first observed in mid-2019 and continued infecting organisations throughout 2020.
- Since 2023, Igor Turashev is wanted by the German authorities for his involvement in DoppelPaymer ransomware.
- The remaining Evil Corp group, led by Yakubets and Ryzhenkov, began developing a new ransomware that would eventually become WastedLocker.

Timeline of Evil Corp's Activity

December 2019: US/UK Disruption

- Following operational support from the NCA, the US Treasury Office for Foreign Assets Control (OFAC) designated Evil Corp and a number of its members. The US Department of Justice also announced indictments and State Department rewards for information leading to the arrest of Maksim Yakubets and Igor Turashev.
- The disruptions in 2019 brought significant cost and risk to the group's operations and bred mistrust and paranoia.

2020: Obfuscation and Evasion - WastedLocker

- Evil Corp were forced to transform their modus operandi to further obfuscate their activities. This included no longer using Dridex and switching to initial access tool SocGholish.
- The individuals became more secretive, abandoning online accounts and restricting their movements.
- Despite attempts to obfuscate their activities, Evil Corp were attributed to the WastedLocker ransomware strain, which they started deploying in mid-2020.

2020-2021: Hades, Phoenix Locker, PayloadBIN and Macaw

- Evil Corp continued to adapt and change their ransomware strains. They developed and deployed further ransomware strains Hades, Phoenix Locker, PayloadBIN and Macaw, all of which shared a similar codebase.
- One of the notable attacks using Phoenix Locker resulted in a $40 million ransomware payment, the largest ever recorded at the time.

2022-2024: Diversification and Affiliation to LockBit

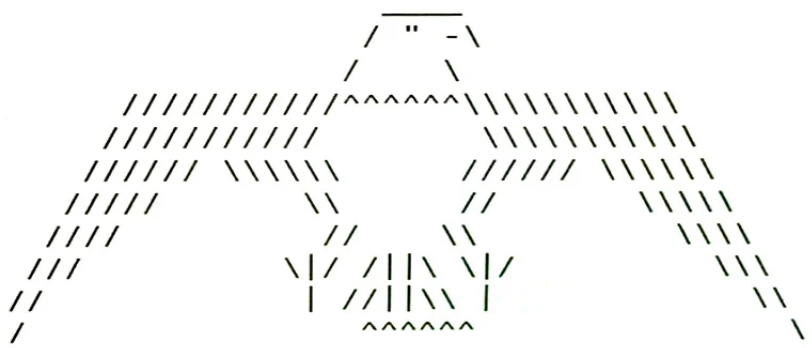
- Whilst many original members are suspected to have gone on to other activity, some remaining Evil Corp members and affiliates have been involved in deploying other ransomware strains since 2022, including LockBit, continuing to employ SocGholish as an initial access tool.
- The NCA have determined that Aleksandr Ryzhenkov, Yakubets' right-hand man, is a LockBit affiliate and has been involved in LockBit ransomware attacks against numerous organisations.
- LockBit ransomware was disrupted by a NCA-led international law enforcement takedown in February 2024 under Operation Cronos.
- Other members of the group continue to operate within the Russian Federation. For example, in December 2022, Igor Turashev and his company came third in a hackathon organised by the Wagner group.

Conclusion

Evil Corp's story is a prime example of the evolving threat posed by cybercriminals and ransomware operators. In their case, the activities of the Russian state played a particularly significant role, sometimes even co-opting this cybercrime group for its own malicious cyber activity.

Born out of a coalescing of elite cybercriminals, Evil Corp's sophisticated business model made them one of the most pervasive and persistent cybercrime adversaries to date. After being hampered by the December 2019 sanctions and indictments, the group have been forced to diversify their tactics as they attempt to continue causing harm whilst adapting to the changing cybercrime ecosystem.

In 2024, further action taken against Evil Corp by the United Kingdom, United States and Australian governments proves their attempts have not gone unnoticed and will not go unchallenged.



NCA
National Crime Agency

The information contained within this paper derives from a number of sources including law enforcement intelligence, NCSC Assessment, reporting from private industry and open source material.